UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,676	06/12/2006	John Alan Gervais	PU030342	4964

24498 7590 06/22/2010

Robert D. Shedd, Patent Operations
THOMSON Licensing LLC
P.O. Box 5312
Princeton, NJ 08543-5312

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
06/22/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/582,676	GERVAIS ET AL.	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *10-13* is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 November 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the arguments filed on 5 March 2010.

2. Claims 1-13 are pending in the application.

3. Claims 10-13 have been allowed.

4. Claims 1-9 have been rejected.

Response to Arguments

5. Applicant's arguments filed 5 March 2010 have been fully considered but they are not persuasive.

On page 10, the applicant argues that Freeman is directed towards a technique for securely changing encryption keys. The applicant argues that although both use encryption, Freeman's technique has little applicability to the conditional access systems described in the present specification.

The examiner respectfully disagrees. Freeman discloses that once a user has had access to a particular set of encrypted files, several prior art approaches exist for securely removing that access. These prior art approaches include: 1) changing the key-pair for the cryptographic file-set, 2) changing the symmetric encryption key for new writes, and 3) re -encrypting the entire file-set for which access rights have changed. Each of these approaches has drawbacks. Simply changing the key-pair that encrypts the symmetric file encryption key is not secure because no means exists for verifying that a user did not cache the symmetric file encryption key, which would allow access not only to previously stored information, but new information as well. Changing the symmetric encryption keys that are used for newly stored information provides some protection, but a user can still access all of the previously stored information in the

cryptographic file-set. This solution has the additional disadvantage that there may eventually be many encryption keys needed to read a single file, which makes the system overly complex. The most secure solution is to re-encrypt the entire cryptographic file system when a user's access to the file-set is removed. While the most secure, this method is also very costly, especially if user access rights change frequently. A Secure Key Replacement Protocol (SKRP), as described below, provides a safe and convenient way to change access rights [0030].

On page 11, the applicant argues nowhere does March teach or suggest that the feature of an access card having a write-once memory and paired with a destination device.

The examiner respectfully disagrees. March teaches a write-once memory [0037]. March teaches that the data can only be written into the memory device by only the manufacturer of the device [0025]. Therefore, the manufacturer is paired with the memory device.

On page 12, the applicant argues that Freeman fails to disclose or suggest conditional access data and conditional access certificates.

The examiner respectfully disagrees. As discussed above, Freeman discloses conditional access data. Freeman discloses that the certificate has a validity date [0028]. Since the certificate has a validity date (conditional time), Freeman discloses conditional access certificates.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 4-6, 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman US 2005/0123142 A1 in view of March et al US 2003/0028734 A1 (hereinafter March).

As to claim 1, Freeman discloses a device, comprising:

a removable digital memory including a port at which digital information stored on the removable digital memory can be accessed (i.e. In an embodiment, the means 297 to prevent a replay attack includes a program 298, operable to read a time stamp on the SKR request and to compare the time stamp to a current time. In another embodiment, the means 292 to prevent a replay attack includes a memory 299 that stores identities of previously deleted private keys and a program 298' that compares the identity of the private key to be replaced with the identities of the previously deleted private keys.) [0031];

a memory for storing first conditional access data and at least one content encryption key (i.e. Once a user has had access to a particular set of encrypted files, several prior art approaches exist for securely removing that access. These prior art approaches include: 1) changing the key-pair for the cryptographic file-set, 2) changing the symmetric encryption key for new writes, and 3) re-encrypting the entire file-set for which access rights have changed. Each of these approaches has drawbacks. Simply changing the key-pair that encrypts the symmetric file encryption key is not secure because no means exists for verifying that a user did not cache the symmetric file encryption key, which would allow access not only to previously stored information, but new information as well.

Changing the symmetric encryption keys that are used for newly stored information provides some protection, but a user can still access all of the previously stored information in the cryptographic file-set. This solution has the additional disadvantage that there may eventually be many encryption keys needed to read a single file, which makes the system overly complex. The most secure solution is to re-encrypt the entire cryptographic file system when a user's access to the file-set is removed. While the most secure, this method is also very costly, especially if user access rights change frequently. A Secure Key Replacement Protocol (SKRP), as described below, provides a safe and convenient way to change access rights.) [0030];

a second port for receiving user certificate data and a first key of a key pair contained in an access card (i.e. The hardware token 400 includes a certificate and private key storage 410, a secure key management JAVA applet 420, and a token key section 430 including a token private key (TK_PRV) 432 and a certificate authority (CA) public key (CA_PUB) 464. Information from the token 400 is transmitted over web browser 375 to certificate authority (CA) 450. The CA 450 may reside at the security server 320, or at an Internet web site, such as the web site 372 (see FIG. 4B). The CA 450 includes a certificate key section 460 having a token public key (TK_PUB) 434 corresponding to the token 400 and a CA private key (CA_PRV) 462.) [0053]; and

a processor responsive to the user certificate data received on the second port for authenticating the received certificate data based on the first conditional

> access data stored in the memory (i.e. FIG. 7 is a flowchart illustrating a secure rekey replacement protocol 500, as executed on the network 300 of FIG. 5. The protocol 500 begins in block 501. In block 510, the CA 450 generates a SKRP rekey request 470. The rekey request 470 includes the challenge 471, the SKRP private key 473, and the key identifier 475 of the private key to be replaced. The CA 450 sends the rekey request 470 to the computer 310. In block 520, the computer 310 receives and processes the rekey request 470. In block 530, the JAVA applet 420, loaded on the token 400, verifies that the rekey request 470 is authentic by comparing the signature on the rekey request 470 to the CA's signature stored on the certificate & private key storage 410.) [0060].

Freeman does not teach that the access card has a write once memory and has been paired with a destination device.

March teaches write once memory and pairing with a destination device [0037, 0060].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman so that the access card would have been write once memory and been paired with a destination device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman by the teaching of March because it provides a method for permanently preventing modification of data stored in a memory device [0004].

As to claim 4, Freeman teaches that the first key is a public key of a public/private key pair [0019].

As to claim 5, Freeman teaches that the access card is inserted into a slot of the device [0017].

As to claim 6, Freeman discloses an access card for enabling secure accessing of digital information stored on a removable memory, the access card comprising:

> a memory having stored therein a first conditional access certificate and a second conditional access certificate (i.e. In an embodiment, the means 297 to prevent a replay attack includes a program 298, operable to read a time stamp on the SKR request and to compare the time stamp to a current time. In another embodiment, the means 292 to prevent a replay attack includes a memory 299 that stores identities of previously deleted private keys and a program 298' that compares the identity of the private key to be replaced with the identities of the previously deleted private keys.) [0031];
>
> means for authenticating first and second conditional access certificates with respective first and second certificate data stored on respective destination and source devices (i.e. Once a user has had access to a particular set of encrypted files, several prior art approaches exist for securely removing that access. These prior art approaches include: 1) changing the key-pair for the cryptographic file-set, 2) changing the symmetric encryption key for new writes, and 3) re-encrypting the entire file-set for which access rights have changed. Each of these approaches has drawbacks. Simply changing the key-pair that encrypts the symmetric file encryption key is not secure because no means exists for verifying that a user did not cache the symmetric file encryption key, which would allow

access not only to previously stored information, but new information as well. Changing the symmetric encryption keys that are used for newly stored information provides some protection, but a user can still access all of the previously stored information in the cryptographic file-set. This solution has the additional disadvantage that there may eventually be many encryption keys needed to read a single file, which makes the system overly complex. The most secure solution is to re-encrypt the entire cryptographic file system when a user's access to the file-set is removed. While the most secure, this method is also very costly, especially if user access rights change frequently. A Secure Key Replacement Protocol (SKRP), as described below, provides a safe and convenient way to change access rights.) [0030];

the memory, following authentication of the card with a destination device, being updated to store a public key of a public/private key pair stored in the destination device (i.e. The hardware token 400 includes a certificate and private key storage 410, a secure key management JAVA applet 420, and a token key section 430 including a token private key (TK_PRV) 432 and a certificate authority (CA) public key (CA_PUB) 464. Information from the token 400 is transmitted over web browser 375 to certificate authority (CA) 450. The CA 450 may reside at the security server 320, or at an Internet web site, such as the web site 372 (see FIG. 4B). The CA 450 includes a certificate key section 460 having a token public key (TK_PUB) 434 corresponding to the token 400 and a CA private key (CA_PRV) 462.) [0053]; and

> a processor operable for, upon authentication of the card with a source device, controlling transmission of the public key to the source device, wherein, in response thereto, the memory being updated to store encrypted data comprising a first key encrypted using the public key, the first key also being used to encrypt information on the removable memory at the source device, whereby communication of the encrypted data to the destination device enables decryption of the data using the private key to recover the first key, to thereby decrypt encrypted information in the removable memory (i.e. FIG. 7 is a flowchart illustrating a secure rekey replacement protocol 500, as executed on the network 300 of FIG. 5. The protocol 500 begins in block 501. In block 510, the CA 450 generates a SKRP rekey request 470. The rekey request 470 includes the challenge 471, the SKRP private key 473, and the key identifier 475 of the private key to be replaced. The CA 450 sends the rekey request 470 to the computer 310. In block 520, the computer 310 receives and processes the rekey request 470. In block 530, the JAVA applet 420, loaded on the token 400, verifies that the rekey request 470 is authentic by comparing the signature on the rekey request 470 to the CA's signature stored on the certificate & private key storage 410.) [0060].

Freeman does not teach that the access card has a write once memory and has been paired with a destination device.

March teaches write once memory and pairing with a destination device [0037, 0060].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman so that the access card would have been write once memory and been paired with a destination device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman by the teaching of March because it provides a method for permanently preventing modification of data stored in a memory device [0004].

As to claim 8, Freeman discloses a digital information destination device comprising:

> a digital information input port (i.e. In an embodiment, the means 297 to prevent a replay attack includes a program 298, operable to read a time stamp on the SKR request and to compare the time stamp to a current time. In another embodiment, the means 292 to prevent a replay attack includes a memory 299 that stores identities of previously deleted private keys and a program 298' that compares the identity of the private key to be replaced with the identities of the previously deleted private keys.) [0031];
>
> a digital information decoder coupled to the digital information input port for decoding digital information encoded with a content encoding key, when the content encoding key is available, to thereby produce unencoded digital information (i.e. Once a user has had access to a particular set of encrypted files, several prior art approaches exist for securely removing that access. These prior art approaches include: 1) changing the key-pair for the cryptographic file-set, 2) changing the symmetric encryption key for new writes, and 3) re-encrypting the entire file-set for which access rights have changed. Each of these approaches has

drawbacks. Simply changing the key-pair that encrypts the symmetric file encryption key is not secure because no means exists for verifying that a user did not cache the symmetric file encryption key, which would allow access not only to previously stored information, but new information as well. Changing the symmetric encryption keys that are used for newly stored information provides some protection, but a user can still access all of the previously stored information in the cryptographic file-set. This solution has the additional disadvantage that there may eventually be many encryption keys needed to read a single file, which makes the system overly complex. The most secure solution is to re-encrypt the entire cryptographic file system when a user's access to the file-set is removed. While the most secure, this method is also very costly, especially if user access rights change frequently. A Secure Key Replacement Protocol (SKRP), as described below, provides a safe and convenient way to change access rights.) [0030];

memory preloaded with at least a second stored User Certificate and mutually corresponding private and public encryption keys associated with the destination device (i.e. The hardware token 400 includes a certificate and private key storage 410, a secure key management JAVA applet 420, and a token key section 430 including a token private key (TK_PRV) 432 and a certificate authority (CA) public key (CA_PUB) 464. Information from the token 400 is transmitted over web browser 375 to certificate authority (CA) 450. The CA 450 may reside at the security server 320, or at an Internet web site, such as the web

site 372 (see FIG. 4B). The CA 450 includes a certificate key section 460 having a token public key (TK_PUB) 434 corresponding to the token 400 and a CA private key (CA_PRV) 462.) [0053];

a content encoding key decryptor for decrypting the content encoding key with a content encoding key encryption key [0027];

an access card reader for reading an access card, where the access card includes authentication means and a memory which, prior to a first insertion in the destination device, includes at least a second Conditional Access Certificate and a first User Certificate and which, after the first insertion (i.e. FIG. 7 is a flowchart illustrating a secure rekey replacement protocol 500, as executed on the network 300 of FIG. 5. The protocol 500 begins in block 501. In block 510, the CA 450 generates a SKRP rekey request 470. The rekey request 470 includes the challenge 471, the SKRP private key 473, and the key identifier 475 of the private key to be replaced. The CA 450 sends the rekey request 470 to the computer 310. In block 520, the computer 310 receives and processes the rekey request 470. In block 530, the JAVA applet 420, loaded on the token 400, verifies that the rekey request 470 is authentic by comparing the signature on the rekey request 470 to the CA's signature stored on the certificate & private key storage 410.) [0060], includes at least the public portion of the private and public encryption keys and which, prior to a subsequent insertion in the destination device, is inserted into a source device and updated to include a content encoding key encrypted with the key encryption key, whereby the destination device, following the subsequent

> insertion of the access card, has the key encryption key and can decrypt the content encoding key and, using the content encoding key, decode the digital information encoded with the content encoding key [0060].

Freeman does not teach that the access card has a write once memory and has been paired with a destination device.

March teaches write once memory and pairing with a destination device [0037, 0060].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman so that the access card would have been write once memory and been paired with a destination device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman by the teaching of March because it provides a method for permanently preventing modification of data stored in a memory device [0004].

As to claim 9, Freeman discloses a method for securely transferring information from a source device to an external device, the source device having a removable digital memory containing information accessible to the source device, the information contained in the digital memory intended to be protected from unauthorized access, the method comprising:

> receiving at the source device user certificate data from an access device and comparing the user certificate data with a first Conditional Access Certificate stored in memory of the source device for authenticating the certificate data (i.e. receiving the certificate, module 222 verifies that the licensing authority is itself trustworthy. Module 222 verifies that the licensing authority is trustworthy by establishing a "chain" of one or more certificates ranging from the licensing

authority up to a root certificate. System 220 maintains a root certificate for each licensing authority that system 220 trusts. Each root certificate is a self-signed certificate that is implicitly trusted by system 220. Upon receipt of the smart card certificate 276, module 220 attempts to establish a chain of certificates from the certificate 276 up to one of the trusted root certificates. This chain may include one or more "intermediate" certificates. Each certificate in the chain will have a "parent" certificate that can cryptographically verify the authenticity of the certificate (e.g., by being digitally signed by the parent). Eventually, the chain leads back to a parent certificate that is one of the trusted root certificates. If such a certificate chain can be established by module 222, then the licensing authority is considered trustworthy. However, if such a certificate chain cannot be established, then the licensing authority is not considered trustworthy and module 222 will not descramble and encrypt the media content.) [column 10, lines 22-43];

accessing, by the source device, the information stored in the removable digital memory and encrypting the information stored in the removable digital memory using at least one content encryption key stored in the source device, upon authentication of the certificate data (i.e. Once a user has had access to a particular set of encrypted files, several prior art approaches exist for securely removing that access. These prior art approaches include: 1) changing the key-pair for the cryptographic file-set, 2) changing the symmetric encryption key for new writes, and 3) re-encrypting the entire file-set for which access rights have changed. Each of these approaches has drawbacks. Simply changing the key-pair

that encrypts the symmetric file encryption key is not secure because no means exists for verifying that a user did not cache the symmetric file encryption key, which would allow access not only to previously stored information, but new information as well. Changing the symmetric encryption keys that are used for newly stored information provides some protection, but a user can still access all of the previously stored information in the cryptographic file-set. This solution has the additional disadvantage that there may eventually be many encryption keys needed to read a single file, which makes the system overly complex. The most secure solution is to re-encrypt the entire cryptographic file system when a user's access to the file-set is removed. While the most secure, this method is also very costly, especially if user access rights change frequently. A Secure Key Replacement Protocol (SKRP), as described below, provides a safe and convenient way to change access rights.) [0030];

receiving at the source device a public key from the access device and encrypting the at least one content encryption key using the public key (i.e. The hardware token 400 includes a certificate and private key storage 410, a secure key management JAVA applet 420, and a token key section 430 including a token private key (TK_PRV) 432 and a certificate authority (CA) public key (CA_PUB) 464. Information from the token 400 is transmitted over web browser 375 to certificate authority (CA) 450. The CA 450 may reside at the security server 320, or at an Internet web site, such as the web site 372 (see FIG. 4B). The CA 450 includes a certificate key section 460 having a token public key (TK_PUB) 434

corresponding to the token 400 and a CA private key (CA_PRV) 462.) [0053]; and

transmitting the encrypted content encryption key to enable access of the encrypted information stored on the removable digital memory by an external device communicable with the access device (i.e. FIG. 7 is a flowchart illustrating a secure rekey replacement protocol 500, as executed on the network 300 of FIG. 5. The protocol 500 begins in block 501. In block 510, the CA 450 generates a SKRP rekey request 470. The rekey request 470 includes the challenge 471, the SKRP private key 473, and the key identifier 475 of the private key to be replaced. The CA 450 sends the rekey request 470 to the computer 310. In block 520, the computer 310 receives and processes the rekey request 470. In block 530, the JAVA applet 420, loaded on the token 400, verifies that the rekey request 470 is authentic by comparing the signature on the rekey request 470 to the CA's signature stored on the certificate & private key storage 410.) [0060].

Freeman does not teach that the access card has a write once memory and has been paired with a destination device.

March teaches write once memory and pairing with a destination device [0037, 0060].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman so that the access card would have been write once memory and been paired with a destination device.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman by the teaching of March because it provides a method for permanently preventing modification of data stored in a memory device [0004].

7. Claims 2, 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freeman US 2005/0123142 A1 and March et al US 2003/0028734 A1 (hereinafter March) as applied to claims 1 and 6 above, and further in view of Roskind et al US 2003/0046544 A1 (hereinafter Roskind).

As to claims 2, 3 and 7, the Freeman-March combination discloses an access card, as discussed above.

The Freeman-March combination does not teach means for establishing that the access card is not expired. Freeman does not teach that the means for establishing that the access card is not expired is performed by comparing the current time with a timestamp in the received user certificate data.

Roskind teaches a smart-card [0016] with a digital certificate with an expiration time [0017]. Once the certificate expires, the smart-card becomes useless. Roskin teaches checking these certificates to see if they have expired [0020].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Freeman-March combination so that the certificate would have had an expiration time. Once the certificate expired, the smartcard would have become useless. There would have been means for checking to see if the certificate had expired.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Freeman-March combination by the teaching of Roskin because the temporary certificates function as a surrogate for the long-term digital certificate and allows the user to immediately remove it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Freeman e the smart card from a card reader and pocket the smart card, thus avoiding the possibility of forgetting the card in a card reader [0012].

Allowable Subject Matter

8. Claims 10-12 are allowed.

As to claim 10, prior art does not disclose, teach or fairly suggest providing a source device having a removable digital memory and including a first Conditional Access Certificate; providing a destination device having a second stored User Certificate and also including mutually corresponding private and public encryption keys associated with the destination device; providing an access card capable of use with both the source device and the destination device, the access card including a second Conditional Access Certificate and a first User Certificate stored therein; placing the access card in the access card port of the destination device a first time; after the placing of the access card in the destination device a first time, accessing the second User Certificate from the destination device, and, within the access card, authenticating the second User Certificate from the destination device with the second Conditional Access Certificate to determine if the public encryption key should be read from the destination device and stored in the access card; if the public encryption key of the destination device should be written to the access card, writing the public encryption key from the

destination device to the access card; removing the access card from the destination device after the writing of the public encryption key; inserting the access card into the source device, and authenticating the first User Certificate with the first Conditional Access Certificate to determine if the access card is valid; if the access card is deemed to be valid by the source device, copying the public encryption key from the access card to the source device; at the source device, encrypting at least some of the digital information in the digital memory using at least one content encryption key to produce encrypted information, using the public encryption key from the destination device to encrypt the content encryption key to thereby generate at least one encrypted content encryption key, and storing the at least one encrypted content encryption key in the access card; connecting the port of the digital memory to the digital information port of the destination device; placing the access card in the access card port of the destination device a second time; after the step of placing the access card in the access card port of the destination device a second time, copying the at least one encrypted content encryption key from the access card to the destination device, and decrypting the encrypted content encryption key using the private key; and at the destination device, receiving the encrypted information from the digital memory, and using the content encryption key to decrypt the encrypted information.

As to claim 13, prior art does not disclose, teach or fairly suggest a memory having at various times at least first, second, and third states; authenticating means; the memory comprising, in the first state, a second Conditional Access Certificate and a first User Certificate stored therein; the memory, in the second state, following a first insertion of the card and first authentication, where the first insertion of the card is into an access card port of a digital information destination device including digital information port which is capable of receiving

the digital information, a second stored User Certificate and mutually corresponding private and public encryption keys associated with the destination device, and the first authentication is performed by the authenticating means authenticating the second User Certificate from the destination device with the second Conditional Access Certificate, comprising the public encryption key from the destination device; the memory, in the third state, following a second insertion of the card and second authentication, where the second insertion of the card is into an access card port of a digital information source device including a removable digital memory containing digital information and a further memory containing a first Conditional Access Certificate and at least one content encryption key, and also following authentication of the first User Certificate stored in the memory of the access card with the first Conditional Access Certificate stored in the source device to establish validity of the access card to the source device, comprising the at least one content encryption key encrypted with the public encryption key.

Any claims not directly addressed are allowed on the virtue of their dependency.

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Primary Examiner, Art Unit 2431